

# フルサービスリゾルバにおける DNSブロッキング・フィルタリングの法的解釈と実施状況



2025年7月3日  
NTTドコモビジネス株式会社  
末松 慶文

# 自己紹介

名前：末松 慶文

2025/7/1から  
社名が変更となりました

2024/6/1から所属

所属：NTTドコモビジネス株式会社 (旧 NTTコミュニケーションズ株式会社)、DNSOPS.jp幹事

業務：ISPとして提供しているフルサービスリゾルバ(キャッシュDNS)と  
権威DNSの設計および開発 (回線サービス名：OCN)

# はじめに

つながろう。驚きを。幸せを。

 **docomo Business**

児童ポルノブロッキング  
を例に

## ■ 本日の内容

- ブロッキングの技術的な仕組み
  - ・ ブロッキング手法
  - ・ DNSブロッキングの実装方法
  - ・ オーバードロッキング
- DNSブロッキングの実効性
- OCNでの実装と運用
  - ・ マルウェア不正通信ブロックサービス
  - ・ 児童ポルノブロッキング

方式の名称やサービス  
名称については、  
この限りではありません

## ■ ここでの用語の定義

ブロッキング : ユーザの同意を得ることなく、アクセスを遮断する措置

フィルタリング : ユーザの同意を得て、アクセスを遮断する措置

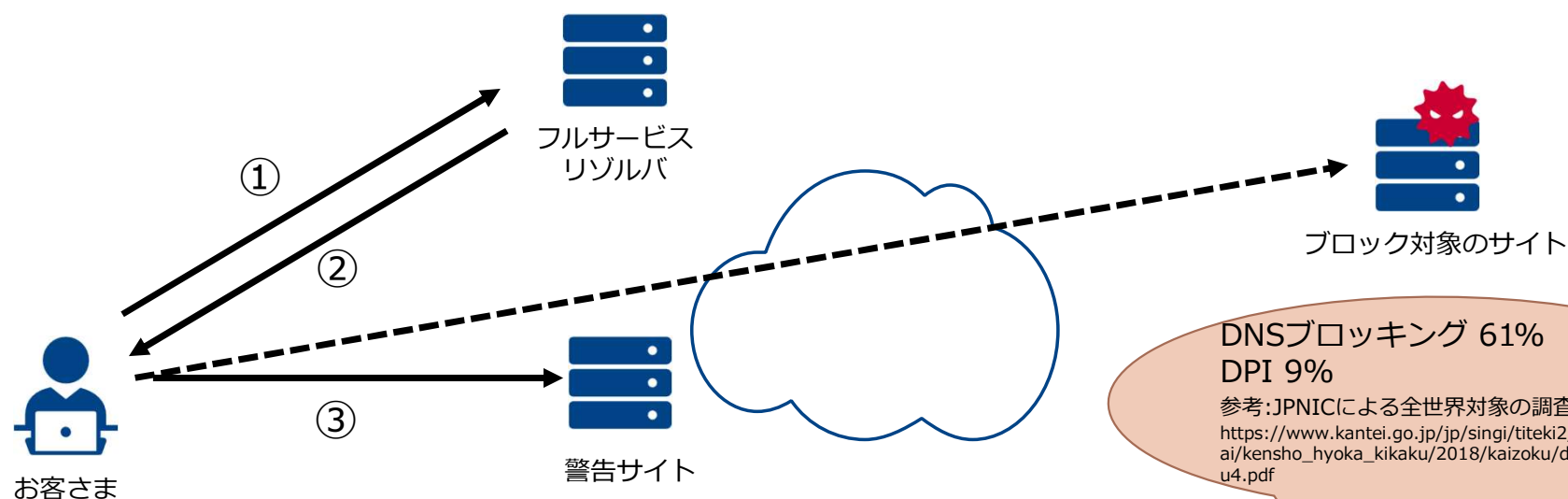
## ■ 免責事項

**発表内容は個人の見解であり、所属する組織の見解やソフトウェア開発元の見解を示すものではありません**

# ブロッキングの技術的な仕組み

# DNSブロッキング方式

- 仕組み：フルサービスリゾルバへの名前解決の要求に対して、警告サイトのIPアドレスを応答することで、ブロック対象サイトへのアクセスをブロッキング
- 費用：既存の設備(フルサービスリゾルバ)を活用することで費用を抑えることが可能
- 精度：ドメイン名に基づいてブロッキングするため、URL情報に基づくブロッキングが可能な方式と比較した場合に精度が低い
- 実効性：ブロッキングを回避し、ブロック対象であるサイトの閲覧が容易（後述）



DNSブロッキング 61%  
DPI 9%

参考: JPNICによる全世界対象の調査(2018)  
[https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho\\_hyoka\\_kikaku/2018/kaizoku/dai3/siryo\\_u4.pdf](https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai3/siryo_u4.pdf)

精度や実効性に課題はあるが、費用とのバランスからDNSブロッキングを選択するISPが多い

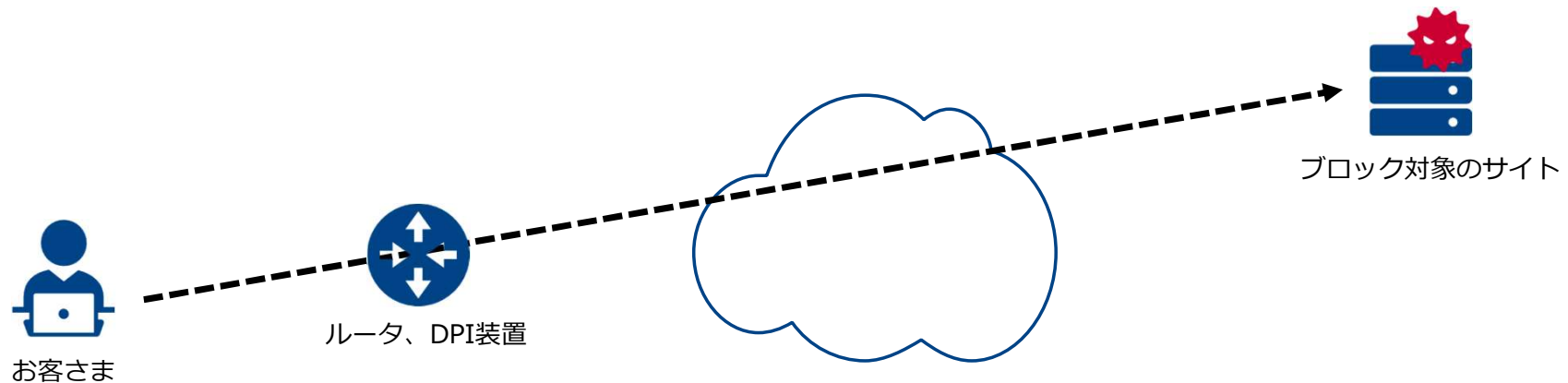
# パケットフィルタリング方式

仕組み(ルータ) : IPヘッダ内の宛先IPアドレスに基づいてブロック

仕組み(DPI) : HTTPコンテンツ部に含まれるURL情報に基づいてブロック

費用 : DPI装置の新規導入は費用大、ルータは費用小

精度 : DPI装置でのブロックは、URL情報に基づくブロックが可能で高精度



## 運用上の課題

エッジルータでのブロックの場合 : 大量の機器への設定が必要

バックボーンルーターでのブロックの場合 : オペミス時の影響が甚大

DPI装置を使用した場合は精度の高いブロックが可能、DNSブロック方式よりも費用大

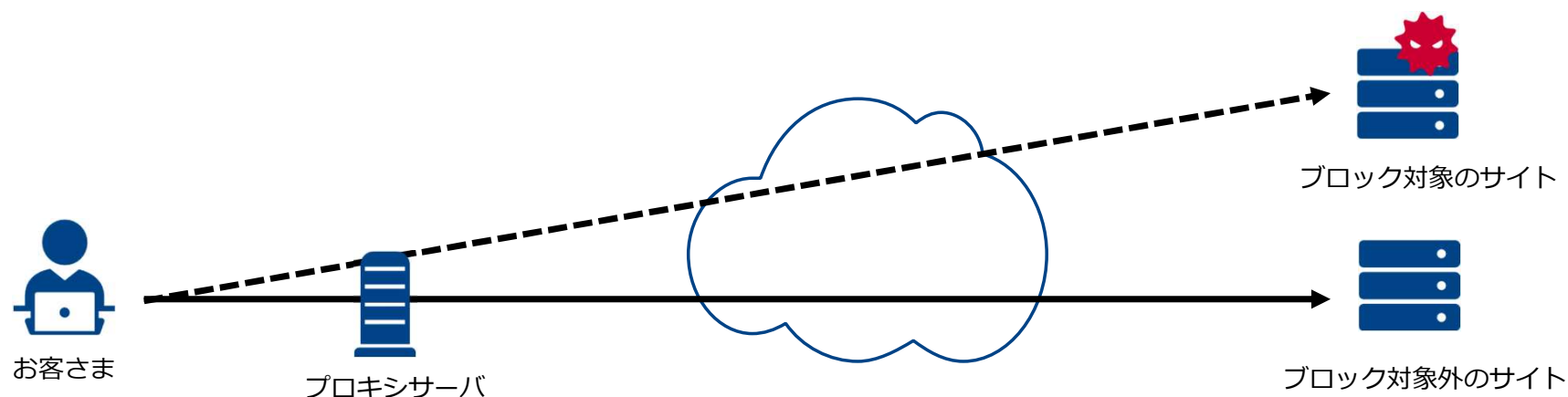
# プロキシ方式

仕組み：URL情報に基づいてHTTPプロキシでブロック

お客さま側での設定を不要とするためには、透過型プロキシとして動作させる必要がある

費用：大規模なプロキシが必要となるため費用大

精度：URL情報に基づくブロックが可能で高精度



精度の高いブロックが可能、DNSブロック方式よりも費用大

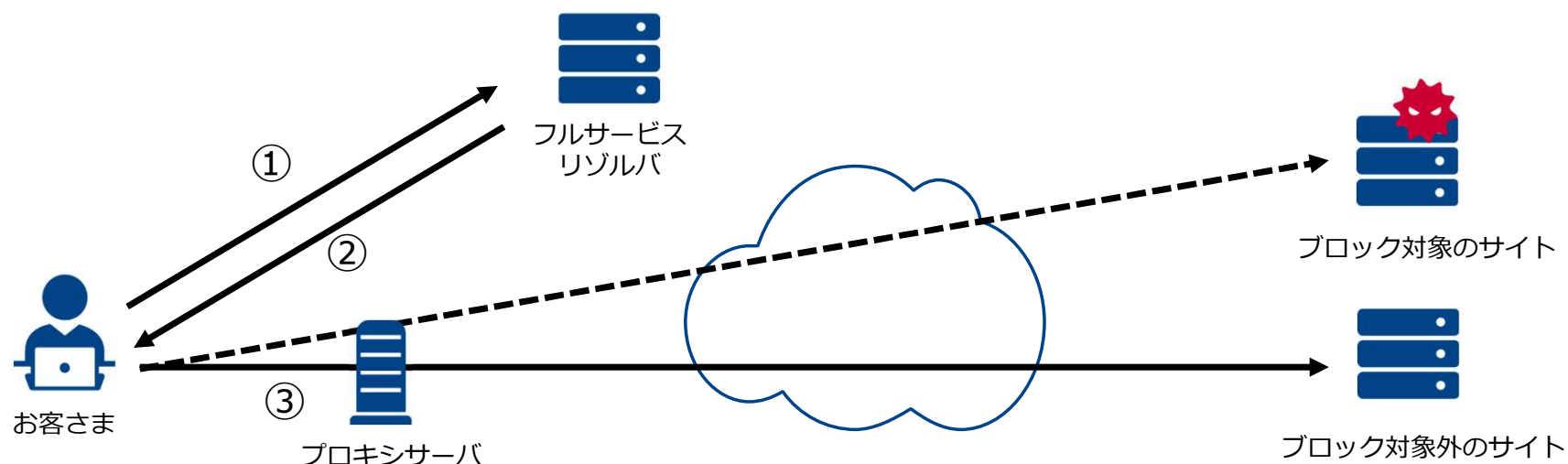
# ハイブリッドフィルタリング方式

仕組み：フルサービスリゾルバに対して疑わしいドメインの名前解決要求があった場合はプロキシサーバのIPアドレスを応答する。プロキシサーバでは、URL情報に基づきブロッキング

（疑わしいIPアドレスベースでプロキシサーバへ経路制御する別方式も存在する）

費用：プロキシ方式と比較して費用の低減が可能

精度：URL情報に基づくブロッキングが可能で高精度



高精度なブロッキングが可能、プロキシ方式より費用の低減が可能

# DNSブロッキングの実装方法

## ■ゾーン上書き方式

- ・ブロック対象のドメイン名をゾーンとして定義し、応答を上書き
- ・rndc reconfigで反映

## ■Response Policy Zones (RPZ)方式

- ・ゾーン転送により、他のサーバとポリシーを容易に共有可能
- ・rndc reloadで反映
- ・5種類のトリガーと6種類のアクションで柔軟に応答をカスタマイズ可能 (BIND 9.18)

参考 : <https://bind9.readthedocs.io/en/v9.18.31/chapter6.html#dns-firewalls-and-response-policy-zones>

- 実装方法 (特定のIPアドレスに応答する場合)

named.conf

```
options { response-policy {zone "block.zone"; }; };  
zone "block" { type master; file "block.zone"; };
```

block.zone(抜粋)

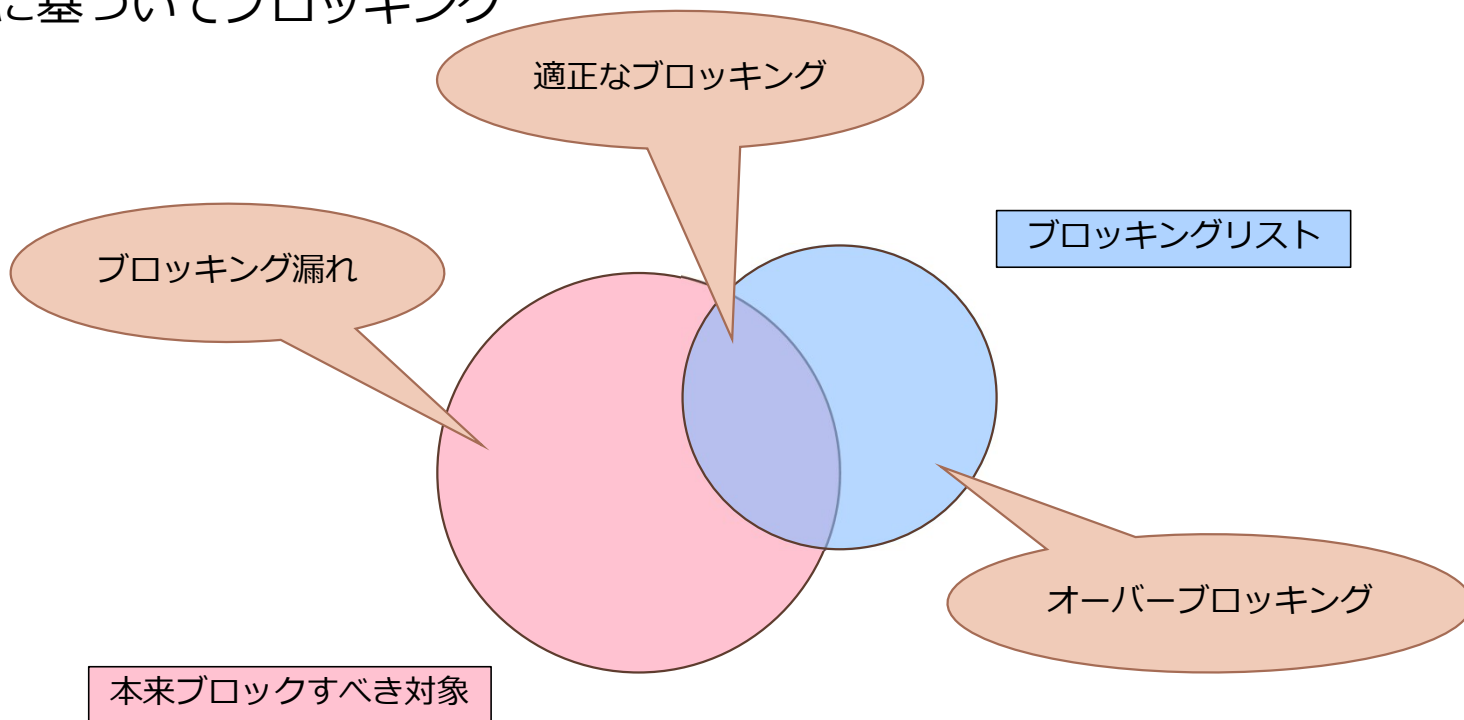
|                   |    |   |           |
|-------------------|----|---|-----------|
| target.example.jp | IN | A | 192.0.2.1 |
|-------------------|----|---|-----------|

# オーバブロック

ブロック対象外を  
誤ってブロック

## ■ オーバブロックとなりえる例

- ・ URLに基づいたブロック用のリストをDNSブロックで使用
- ・ ブロック対象と対象外のコンテンツが同一IPアドレスで提供されている状況下でIPアドレスに基づいてブロック



オーバブロックの防止には、正しいリストを正しく適用することが重要

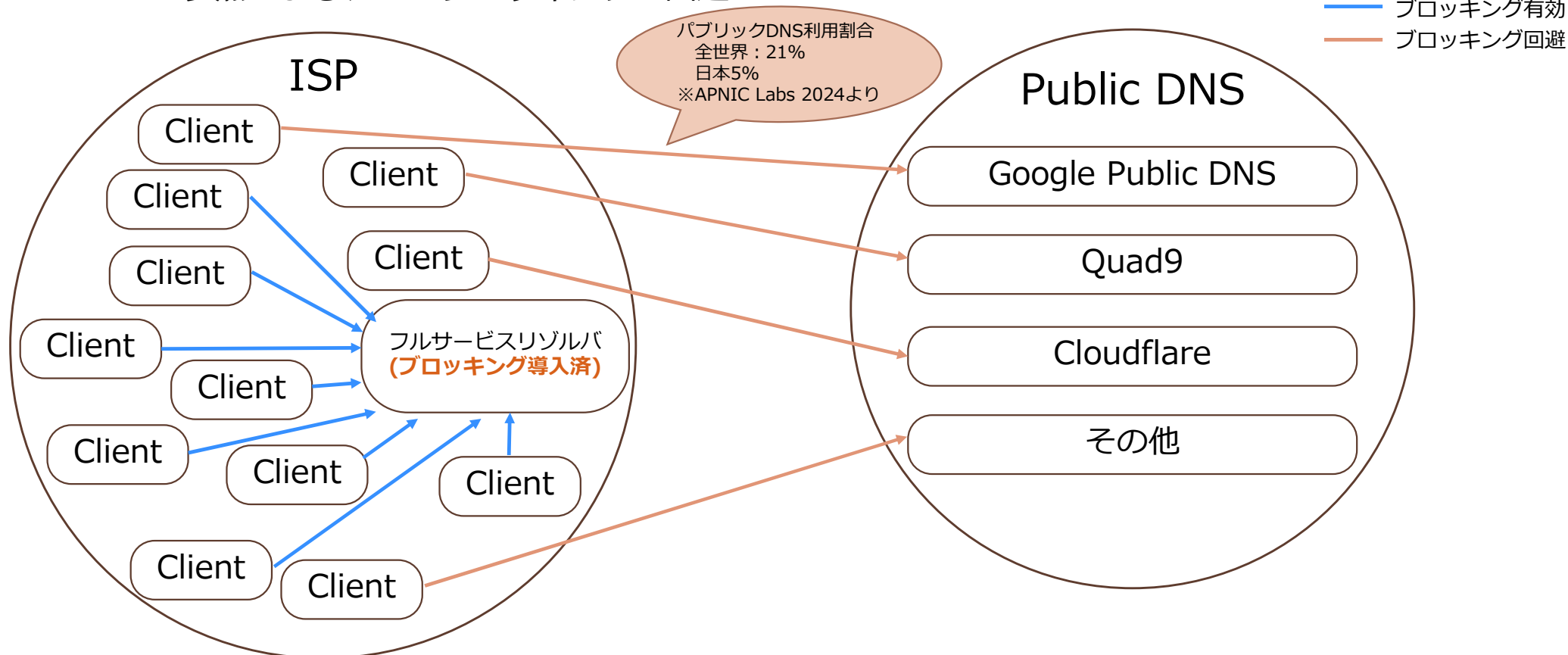
# DNSブロッキングの実効性

# DNSブロッキングの実効性

つながる。驚きを。幸せを。

 docomo Business

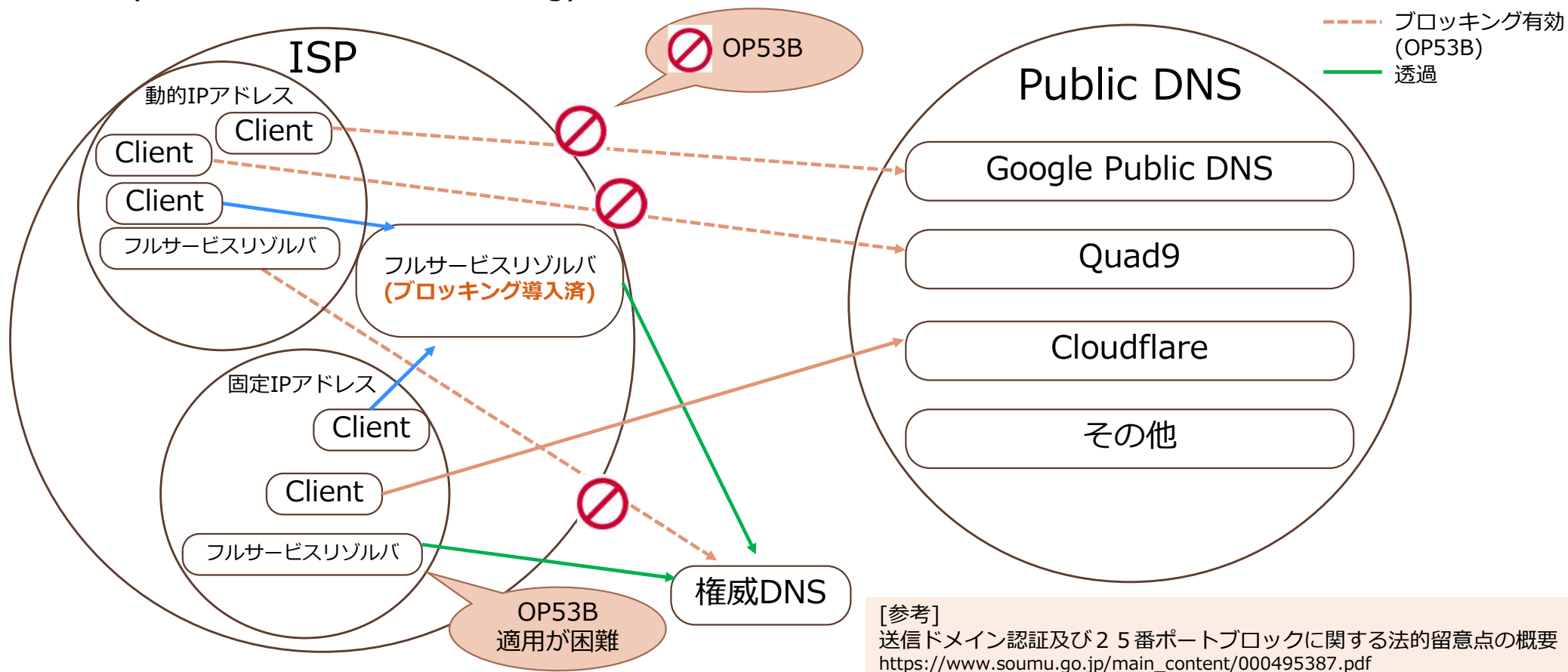
## ■ Public DNS参照による、DNSブロッキングの回避



ブロック対象であるサイトの閲覧が容易であり、ブロッキングの実効性に課題

# DNSブロッキング回避の対策

## ■ OP53B (Outbound Port 53 Blocking)



OP25Bは正当業務行為として法的な整理がされているが、OP53Bは法的な整理がされていない

# OCNでの実装と運用

# マルウェア不正通信ブロックサービス (OCN)の仕様

## ■ サービス概要

OCNのネットワーク上で、お客さまのPCやスマートフォンなどの端末がマルウェアに感染したことにより発生するC&Cサーバへの通信を検知し、OCN側で自動的に遮断するサービス

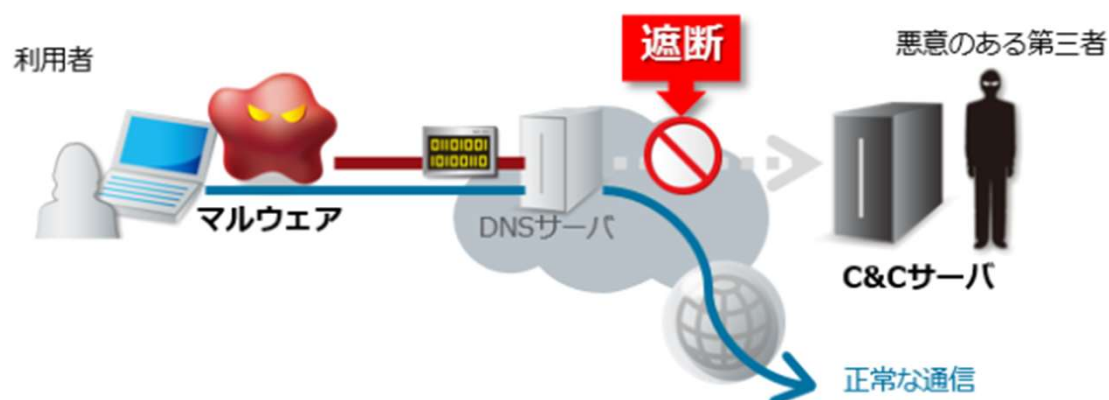
## ■ 特徴

- ・ お申込み不要
- ・ 設定不要
- ・ 利用料金無料

- ・ 契約約款に基づく事前の包括同意
- ・ オプトアウトの整備

### サービス 利用時

「マルウェア不正通信ブロックサービス」は、マルウェアが外部のC&Cサーバとの通信を行おうとすると、未然に遮断します。



【個人のお客さま向け】

「マルウェア不正通信ブロックサービス」

<https://service.ocn.ne.jp/ocn-security/info/malware.html>

【企業のお客さま向け】

・ 企業向けOCNをご利用の方はこちら

「マルウェア不正通信ブロックサービス」

<http://www.ocn.ne.jp/business/security/malware/>

・ 「Arcstar Universal One」をご利用の方はこちら

「VPNサービス Arcstar Universal One インターネット接続機能」

[http://www.ntt.com/vpn/data/op\\_internet.html](http://www.ntt.com/vpn/data/op_internet.html)

# マルウェア不正通信ブロックサービス (OCN)

■実装イメージ



当日限り

# マルウェア不正通信ブロックサービス (OCN)

■ オプトアウト実装イメージ

当日限り

# 児童ポルノブロッキング(OCN)の実装

## ■実装イメージ

当日限り

# おわりに

## 技術的な仕組み

- ブロッキング手法
  - ・費用と実効性のバランスからDNSブロッキングを使用する事業者が多い
- オーバーブロッキング
  - ・リストの性質(DNSブロッキング用、URLブロッキング用)を理解し、正しく適用
- DNSブロッキングの実効性
  - ・DNSブロッキングは回避が容易で実効性には限界

## 実施内容と運用状況

- 児童ポルノブロッキング、マルウェア不正通信ブロックサービスの実装と運用

Extended DNS Errors(RFC 8914)を拡張しDNSフィルタリング詳細を通知するInternet Draft

- <https://datatracker.ietf.org/doc/draft-ietf-dnsop-structured-dns-error/>

# 参考

- ・ オンラインカジノに係るアクセス抑止の在り方に関する検討会(第4回)  
[https://www.soumu.go.jp/main\\_sosiki/kenkyu/online\\_casino/02kiban18\\_02000407.html](https://www.soumu.go.jp/main_sosiki/kenkyu/online_casino/02kiban18_02000407.html)
- ・ 電気通人事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ  
[https://www.soumu.go.jp/menu\\_news/s-news/01kiban18\\_01000134.html](https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000134.html)
- ・ 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン  
[https://www.jaipa.or.jp/other/mtcs/guideline\\_v6.pdf](https://www.jaipa.or.jp/other/mtcs/guideline_v6.pdf)
- ・ DNSブロッキングによる児童ポルノ対策ガイドライン  
<https://www.good-net.jp/files/original/201711012219018966761.pdf>
- ・ ISP 技術者サブワーキング 報告書  
<https://www.good-net.jp/files/original/201711012219018064310.pdf>
- ・ ブロッキングと通信の秘密との関係  
[https://www.good-net.jp/investigation/working-group/anti-child-porn\\_category\\_112/blocking/relation/relation\\_2-2](https://www.good-net.jp/investigation/working-group/anti-child-porn_category_112/blocking/relation/relation_2-2)
- ・ インターネットと通信の秘密  
<https://www.slideshare.net/slideshow/iijmio-meeting-20/105851332>
- ・ グローバルなインターネット関連組織を対象とした、各国・地域におけるWebサイトブロッキングに関するアンケート調査実施の情報共有  
[https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho\\_hyoka\\_kikaku/2018/kaizoku/dai3/siryou4.pdf](https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai3/siryou4.pdf)
- ・ 一般社団法人インターネットコンテンツセーフティ協会 統計情報  
<https://www.netsafety.or.jp/news/info/info-042.html>
- ・ インターネット上の海賊版に対する総合的な対策メニュー及び工程表の再更新について  
[https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2024/0528\\_sankou.pdf](https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2024/0528_sankou.pdf)
- ・ ブロッキングにかかわる法制度整備を行う場合の論点について（案）  
[https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho\\_hyoka\\_kikaku/2018/kaizoku/dai6/siryou1.pdf](https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai6/siryou1.pdf)
- ・ Response Policy Zone (RPZ)  
<https://www.isc.org/rpz/>
- ・ Tutorial on Configuring BIND to use Response Policy Zones (RPZ)  
[https://www.isc.org/docs/BIND\\_RPZ.pdf](https://www.isc.org/docs/BIND_RPZ.pdf)

つなごう。驚きを。幸せを。



ご清聴ありがとうございました